Print Form

Information System Profile

Contractor:

Address:

Cage Code:

IS Number:

This IS Profile is associated with ODAA Unique Identifier:

IS Profile Revision Log		
Revision	**Description of Baseline Change**	**Dates**

The following attachments are included with this template.

- Configuration Management Documentation
  - Hardware Baseline (required)
  - Configuration Diagram (required)
  - Software Baseline (required)
- DSS Form 147, Record of Approval for Closed Area (required for Closed Area)
- IS Security Seal Log (for Restricted Areas, if needed)
- Sample Maintenance, Operating System & Security Software Change Log (required)
- Sample Briefing Acknowledgement Form (required)
- Upgrade/Downgrade Procedures (required for Periods Processing)
- Trusted Download Procedures (required for Trusted Downloads)
- DSS Configuration Tool Output Report or ISSM System Certification Test Checklist (required)
- Sample Relocation Letter (required for Mobile Systems to Government Site)

Protection, Sensitivity Level, and User Information	
Protection Level ☐ **1** ☐ **2** **Highest classification level of data:** ☐ Confidential, Basic Confidentiality Level of Concern ☐ Secret, Medium Confidentiality Level of Concern ☐ Top Secret, High Confidentiality Level of Concern **Category(s) of Info:** ☐ COMSEC ☐ RD ☐ FRD ☐ FGI ☐ Other: **Formal access approvals:** ☐ No ☐ Yes. If yes, indicate ☐ NATO ☐ CNWDI ☐ Crypto	**Levels of Concern**: Integrity ☐ High ☐ Medium ☐ Basic ☒ Not Contractually Imposed Availability ☐ High ☐ Medium ☐ Basic ☒ Not Contractually Imposed **Minimum clearance level of users:**

Information System Profile	IS # ID:	**Contractor facility name:** **CAGE Code:**
Date:	**Facility Address:**	

Contact Information

FSO: **Phone Number:** **Email:**	**ISSM:** **Phone Number:** **Email:**	**ISSO:** **Phone Number:** **Email:**

System Identification

General description of IS hardware and IS configuration:

Contract Number(s) and Program Name(s):

IS Purpose/Usage:

IS Physical Location and Safeguards

Address (if different from facility address):

Building:

Room or Column #:

Type of Area:

☐ Closed Area, See attached DSS form 147

☐ Restricted Area (check all that apply): ☐ Defined Perimeter Boundary ☐ Locked Room or Cabinet ☐ Security Seals ☐ Other (describe):

For Restricted Areas only: Describe in use protections to prevent viewing or disclosure of classified information to unauthorized persons:

Special Procedures

Other Special procedures: ☐ N/A ☐ Yes If yes, describe:

Other Comments or Additional Information:

This page is not applicable

HARDWARE BASELINE

System	Device Type	Manufacturer/Model	Unique ID[1]	Memory/Media Size and Type[2]	Clearing/Destruction Procedure[3]

Note 1 – Provide a unique identifier (e.g. serial number, barcode #) for any device that retains classified information when all power is removed.
Note 2 – List the size/capacity of any memory or media that retains classified information when all power is removed.
Note 3 – If the device has all volatile memory, specify Power Off in this column. If more lengthy sanitization or write-protection methods are used, specify the attachment # in the Protection Profile that includes the sanitization or write-protection procedure.

IS Profile Attachment 1

☐ This page is not applicable

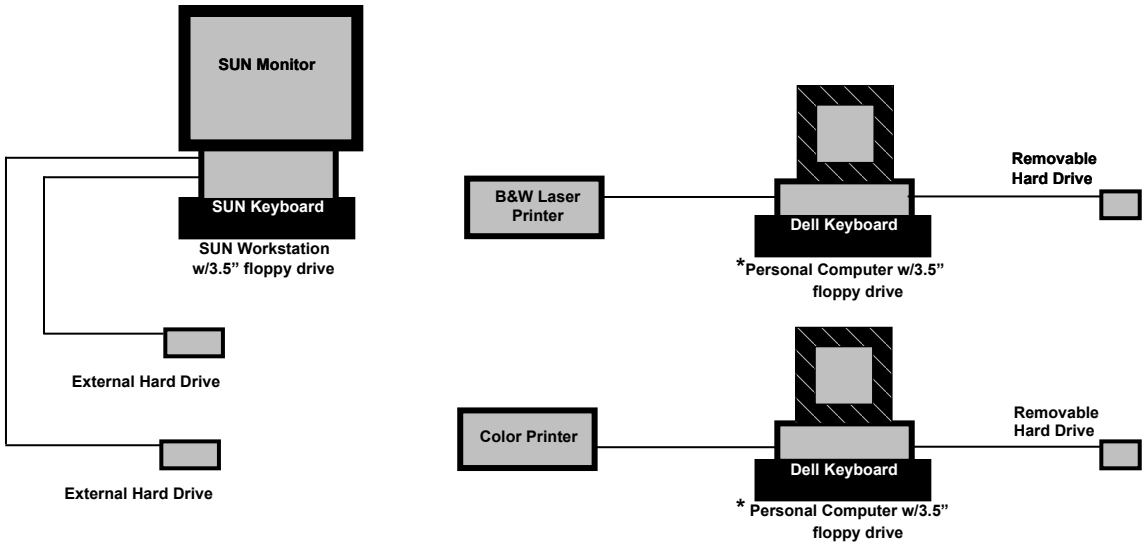
HARDWARE BASELINE

System	Device Type	Manufacturer/Model	Unique ID[1]	Memory/Media Size and Type[2]	Clearing/Destruction Procedure[3]

Note 1 – Provide a unique identifier (e.g. serial number, barcode #) for any device that retains classified information when all power is removed.
Note 2 – List the size/capacity of any memory or media that retains classified information when all power is removed.
Note 3 – If the device has all volatile memory, specify Power Off in this column. If more lengthy sanitization or write-protection methods are used, specify the attachment # in the Protection Profile that includes the sanitization or write-protection procedure.

IS Profile Attachment 1

CONFIGURATION DIAGRAM



*** Devices may be used as standalone without connection to LAN.**

THIS DIAGRAM IS AN EXAMPLE. YOU MUST CREATE A DIAGRAM FOR THE IS IDENTIFIED IN THIS PROFILE

IS Profile Attachment 2

Click on example to upload diagram image file.

SOFTWARE BASELINE

Software Name	Vendor	Version # or Release

IS Profile Attachment 3

This list must include all security relevant software (example: audit, antivirus, and sanitization software) and operating system software.

☐ This page is not applicable

SOFTWARE BASELINE

Software Name	Vendor	Version # or Release

IS Profile Attachment 3

This list must include all security relevant software (example: audit, antivirus, and sanitization software) and operating system software.

RECORD OF CONTROLLED AREA

(May also be used for recording approval of vaults and strong rooms)

1. TYPE:
   - ☐ Closed
   - ☐ Vault
   - ☐ Spec. Container

   Class:
   - ☐ A
   - ☐ B
   - ☐ C
   - ☐ Modular

2. FACILITY NAME AND ADDRESS:

3. IDENTITY OF AREA, NUMBER AND LOCATION:

3a. Normal Hours of operations

4. APPROVED DEGREE OF STORAGE:

4a. Type of Material Safeguarded:

4b. Open Storage:
☐ Yes ☐ No

5. NAME AND TITLES OF FACILITY PERSONNEL CONSULTED:

6. Date of Inspection:

CONSTRUCTION FEATURES

7. WALLS: Do walls extend to true ceiling?
☐ Yes ☐ No

8. DOORS: How many? _____ Entry/Exit _____ Non-Entry/Exit _____
Description:

9. CEILINGS:

9a. If a false ceiling, the ceiling or space above is checked on a (weekly, monthly, biannual) basis or secured as follows:

10. FLOORS:

10a. If a raised floor, the space below or crawl ways are checked on a (weekly, monthly, biannual) basis or secured as follows:

11. WINDOWS: How many? _____ Opaque _____ Non-Opaque _____
Description:

12. MISCELLANEOUS OPENINGS:

13. DOOR LOCKING DEVICES
a. During working hours
b. During non-working hours
c. Non-entry doors

14. SUPPLEMENTAL PROTECTION:
a. Alarm System
(1) Monitor: ☐ Proprietary ☐ Subcontract
(2) Type: ☐ Central ☐ Direct ☐ Local
(3) U.L. (CRZH) Certificate Checked ☐ Yes ☐ No
b. Guards
(1) ☐ Proprietary ☐ Contractor
(2) Frequency of Rounds _____
(3) ☐ Alarm Response Only
c. Security-In-Depth (SID): ☐ Yes ☐ No

15. UNUSUAL FEATURES OF CONSTRUCTION:

SIGNATURE OF IS REPRESENTATIVE(S) APPROVING AREA:

FIELD OFFICE:

SIGNATURE OF FACILITY SUPERVISOR:

DSS Form 147, APR 00

IS Profile Attachment 4
Include in Profile only when applicable.
Click on sample to upload a scanned signed image of this form. Additional images can be uploaded in the back of this IS Profile

IS SECURITY SEAL LOG

Seal No.	Date Seal Applied	Seal Location	Name/Signature of Person Applying Seal	Date Seal Broken	Name/Signature of Person Breaking Seal	Reason for Seal Breaking

IS Profile Attachment 5
Include in Profile only when applicable.

MAINTENANCE, OPERATING SYSTEM & SECURITY SOFTWARE CHANGE LOG

This log is used to record additions, removals, maintenance, and changes to hardware, installation, and testing of O/S & Security Software.

DATE	SYSTEM/DEVICE DESCRIPTION	COMPONENT ID NUMBER	DESCRIPTION OF ACTIONS	PERSON/ (Company if appl)	PCL	ESCORT

All entries must include date, description of action, and person taking action. Company of person performing action is only required if they are not an employee. Escort is only listed when the performing person does not have the requisite clearances and/or Need-To-Know. Personnel Security Clearance (PCL) must be included for entries involving changes to hardware or software. Hardware changes must include system/device description, id number and clear/sanitize actions if applicable.

IS Profile Attachment 6

IS ACCESS AUTHORIZATION AND BRIEFING FORM

Printed Name: _____ Phone: _____

Acknowledgment of Briefing

I understand that as an information systems (IS) user, it is my responsibility to comply with all security measures necessary to prevent any unauthorized disclosure, modification, or destruction of information. I have read or will read all portions of the System Security Plan (SSP) pertaining to my level of responsibilities and agree to the following:

1. Protect and safeguard information in accordance with the SSP.
2. Sign all logs, forms and receipts as required.
3. Obtain permission from the ISSM or designee prior to adding/removing/or modifying any system hardware or software.
4. Ensure all files and media are checked for viruses and malicious logic using a current virus detection tool prior to, or at the time of introduction to an IS.
5. Escort non-authorized personnel in such a manner as to prevent their access to data they are not entitled to view.
6. I will comply with the following password requirements:
   a) I will select a password that is a minimum of 14 non-blank characters. The password I select will contain at least one number or punctuation symbol and a combination of upper and lower alpha characters.
   b) Protect system passwords commensurate with the level of information processed on the system and never disclose to any unauthorized persons.
   c) If I have access to a generic or group account, I will first login with my personal user id prior to accessing the generic/group account.
7. Protect all media used on the system by properly classifying, labeling, controlling, transmitting and destroying it in accordance with security requirements and security classification guide.
8. Protect all data viewed on the screens and/or outputs produced at the level of system processing until it has been reviewed.
9. I understand I must be authorized in writing by the ISSM to perform a trusted download. If authorized, I will perform this in accordance with the trusted download procedures.
10. Notify the ISSM or designee when I no longer have a need to access the system (i.e.: transfer, termination, leave of absence or for any period of extended non-use).
11. Use the system for performing assigned company duties, never personal business.
12. Comply with all software copyright laws and licensing agreements.
13. I understand that all of my activities on the IS are subject to monitoring and/or audit.

Signature Date

FOR SECURITY AND ADMINISTRATOR USE ONLY

☐Employee ☐Visitor/Company: _____ Visit request expires on: _____

Clearance/ Special Briefings: _____ Verified By: _____

Account Name: _____ Date Added: _____

Type of Account: ☐ General ☐ Privileged

Other Access/Privileges, or Comments: _____

Date Account Disabled/Deleted: _____

UPGRADE DOWNGRADE PROCEDURE/RECORD

UPGRADE PROCEDURES

1. Clear area of unauthorized persons and verify classified processing sign is posted.
2. Obtain classified media from approved storage.
3. Inspect Security Seals.
4. Install classified drive(s).
5. Boot system.
6. Document upgrade action below.

DOWNGRADE PROCEDURES

1. Verify classified material has been removed from printer(s).
2. Verify classified hard drive, CDs, and Floppy Disks are removed.
3. Shutdown, power down system for 30 seconds.
4. Document downgrade action below.

	UPGRADE			**DOWNGRADE**		
Component or System#	DATE	TIME	PERSON	DATE	TIME	PERSON

Include in Profile only when applicable.
IS Profile Attachment 8

☐ This page is not applicable

TRUSTED DOWNLOAD

Background

Trusted download refers to a procedure, or series of procedures, that permits information to be released below the accredited level of the Information System (IS).

Almost without exception, the majority of contractors Information Systems that are accredited to process classified information operate at Protection Level (PL) 1 or PL 2. As such, the protection requirements identified in Section 6 of NISPOM Chapter 8 do not support more than one classification and/or sensitivity level of information. Simply stated, the IS cannot recognize or distinguish information based on content. All information residing or processed on a PL 1, 2 or 3 IS are handled/treated at the classification/sensitivity level for which the IS is accredited.

Scope

The February 2006 NISPOM Chapter 8 requirements for trusted download shall be implemented by all newly accredited or reaccredited ISs at PL1, PL2, or PL3 that require the transfer of information with different sensitivities or information with unclassified or lower classified information. The implementation of the trusted download requirements will provide contractors with specific guidelines on how to perform this task while maintaining an acceptable level of risk during the creation of lower-than-system-level output.

☐ This page is not applicable

In general, DSS trusted download requirements include:

- A comprehensive review by a "Knowledgeable User" (see definitions)
- The applicable DSS standard file type/formats and file transfer procedures documented in the IS System Security Plan (SSP)
- Where authorized on the DD-254 or as a contract line item, alternate detailed procedures included in the IS SSP which constitutes an acknowledgement and acceptance of additional risk from the government customer/data owner.

NISPOM Requirements

The following Chapter 8 requirements apply to Trusted Downloading:

8-310a. Human-Readable Output Review. An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

8-310b. Media Review. Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. Cognizant Security Agency-approved random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

Definitions

1. Aggregation. The generation of a higher level overall classification of information when combining two or more lower level classified files (e.g. the combination of two unclassified files on a media producing CONFIDENTIAL or SECRET media) based on Security Classification Guide(s), restriction(s).

2. Acknowledgement of Risk. Alternative Trusted Downloading Procedures that do not follow the DSS guidelines may be used only when the Government Customer/data owner has formally (in writing) acknowledged and accepted the risk inherent in the alternate file type/format and procedures.

3. Comprehensive Review. A methodical review to ensure that all higher level information has been removed prior to the data being released outside the IS's security boundary. Comprehensive Reviews fall into two categories: Hardcopy and media. For hardcopy output a review shall be performed by a "Knowledgeable User" to determine the correct classification and portion marking of the information.

☐ This page is not applicable

For large products in human-readable form, the comprehensive review must be done on no less than 20% of the output product. For media output, the media shall be created by a "Knowledgeable User" following the DSS "File Transfer Procedure" as defined in the IS's SSP.

4. Knowledgeable User. An IS user (general or privileged) who is considered a data matter expert with extensive knowledge of all appropriate security classification guide(s), and who can perform the "Comprehensive Review". The User shall be trained by the Information System Security Manager (ISSM) or Information System Security Officer (ISSO) in understanding the vulnerabilities associated with producing lower-than-system-level output and file transfer procedures.

5. Sensitivity. Refers to formal access requirements (e.g., NATO, COMSEC, CNWDI) or caveats that specify handling or releasability restrictions (e.g., Foreign Government Information (FGI).

6. Slack Space. The data storage space that exists from the end of a file to the end of the last cluster assigned to the file. Slack space potentially can contain randomly selected bytes of classified data from computer memory.

7. Trusted download. A procedure, or series of procedures, that permits information to be released below the accredited level of the Information System (IS). Release of information outside the IS may take the form of hardcopy (or human-readable), digital/analog media, or electronic transfer.

File Type/Formatting Issues

The many different file formats represent a security challenge to the contractor, DSS, and in many cases the Government Contracting Activity (GCA) or data owner. For the most part every application, even those belonging to a professional software suite (e.g., Microsoft Office, Mat Lab, Claris) formats, stores, displays, and/or codes information differently. Some use proprietary coding techniques, some hide file related information (in binary and/or ASCII format) within the file, and some do things from a DSS security viewpoint that even the vendor cannot explain. However, to perform a reliable "trusted download", existing file format vulnerabilities must be considered.

While no security procedures can mitigate 100% of the risk involved, the DSS approved Trusted Download procedures mitigate an acceptable amount of risk and have been tested to ensure the reliability of the procedures.

The only "SAFE" method of removing unclassified information from a classified system is to print and perform a comprehensive human review by a "Knowledgeable User". Once the printed output is reviewed, it is a simple process to scan the document into an unclassified or lower classified information system. This will eliminate the vulnerabilities associated with electronic media.

☐ This page is not applicable

No matter which file type/formats are used, the SSP must identify the file format(s) and specific procedures for reviewing and transferring those formats.

Legacy Operating Systems Slack Space Issues

In addition to File Type/Format issues, there is also an issue with how certain Operating Systems handle slack space that must be considered when copying information to media or during electronic transfers. Systems that are known to produce slack space with non-predictable results are:

- MAC (note: does not include MAC X O/S)
- Windows 95
- Windows 95, release A
- Some early versions of Windows 98

When copying to media or performing electronic transfers from these operating systems a DSS-authorized copy product/procedure must be used.

☐ This page is not applicable

DSS Authorized File Type/Formats

This Policy supports both hardcopy and media/electronic transfer file type/formats.

Hardcopy:
All human-readable output sent to hardcopy devices, such as printers, copiers and faxes, independent of the original files format, fall into this category. This includes, but is not limited to, ASCII, HEX and Octal files, word processing, graphics, database and scientific files. As long as the file can be reviewed meeting the "Comprehensive Review" criteria it is eligible for release at a level (i.e., classified or unclassified) lower than the accredited IS level.

Media/Electronic Files:
The following file formats are authorized by DSS to be released from the IS at or below the IS's accreditation level without an acknowledgement of risk from the government customer, but only after a comprehensive review:

Format Type	Explanation	Common File Extension(s)
ASCII	ASCII formatted information is essentially raw text just like the words you're reading now. Many applications have the ability to export data in ASCII or text format. Program source code, batch files, macros and scripts are straight text and stored as ASCII files. ASCII files may be read with any standard text editor.	.**txt .dat .c .for .fil .asc .bat** Note: This is not an all-inclusive list. If a file cannot be read with a standard text editor, try changing the extension to **.txt**. If the file still cannot be read with a text editor, it is most likely not an ASCII file.
Hypertext Markup Language	The document format used on the World Wide Web. Web pages are built with HTML tags (codes) embedded in the text. HTML defines the page layout, fonts and graphic elements as well as the hypertext links to other documents on the Web.	**.html .htm**
JPEG	Joint Photographic Experts Group (pronounced jay-peg) An ISO/ITU standard for compressing still images that is very popular due to its high compression capability.	**.jpg**
BMP	A Windows and OS/2 bitmapped graphics file format. It is the Windows native bitmap format. Every Windows application has access to the BMP software routines in Windows that support it.	**.bmp**
Graphics Interchange Format	A popular bitmapped graphics file format developed by CompuServe.	**.gif**

*Note: Executable programs may not be transferred. The source code (ASCII text) may be reviewed/ transferred to a lower level IS then re-compiled into executable code.

IS Profile Attachment 9

☐ This page is not applicable

DSS File Transfer Procedures

For every file type or format, there are an endless number of transfer procedures that have been developed by industry and government. Some of the more common ones are identified at the end of this document. What's important to remember about these or any alternate procedure is that the contractor must get the GCA or data owner to acknowledge the increased risk to classified information created by using one of the non-DSS authorized file types/formats and/or procedures.

No matter what file format or procedure is used, there are requirements that are common to all general media and to electronic transfers:

1. The file types/formats and transfer procedures must be certified by DSS and documented in the SSP.

2. Target media must be factory fresh.

3. A comprehensive review must be performed so as to ascertain the sensitivity and classification level of the data.

4. Classified path/file embedded links and/or classified path/file name(s) are not used for source or target file(s).

5. The compilation of all files on the target media does not cause an increased classification level due to "Aggregation".

6. File(s) are transferred using a known, authorized utility or command.

7. The target media is verified to contain only intended source file(s).

8. File(s) are verified on target media to contain the correct sensitivity of information and/or level of unclassified or lower classified information.

9. The appropriate security classification label is applied to the target media.

10. An administrative record of the transfer is created and maintained.

If the ISSM is unable to implement the DSS Authorized Procedures, the System Security Plan must include a description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA.

☐ This page is not applicable

DSS Authorized Procedure (Windows-Based)

1. The target media must be new.

2. The procedure must be performed by a "Knowledgeable User".

3. If multiple files are being transferred, create a designated directory for the transfer using the DOS make directory command (md [drive:] path) or the new folder command under Windows Explorer. [Rationale: This will establish an empty directory which helps ensure that only intended files are transferred.]

4. If multiple files are being transferred, transfer all files into the newly created directory.

5. As a general rule, files should be converted to one of the acceptable formats first (DSS Authorized File Type/Formats), then reviewed. Drawings and presentation type files (e.g. PowerPoint, Publisher, and Visio) are an exception. These types of files within their native application may have layers of information, for example text on top of graphics, or multiple graphics layered together. Once exported into one of the authorized graphic formats (i.e. .bmp, .jpg, .gif) the layers will be merged together and will not be editable to remove any higher classified information. To review these files use the native application used to generate the file. Ensure that every page, chart, slide, drawing etc. of the file is examined. Within each page, chart, slide, drawing, etc. ensure that all layers are reviewed by ungrouping and moving objects around so everything is visible. Some applications may also have information in headers and footers, notes pages, etc. Below is a detailed procedure for reviewing one of the more commonly used presentation/ graphic applications, review of MS Word and MS Excel files can follow the same instructions, but some items will not apply:

PowerPoint:

a. Review Headers and Footers. To do this: Click on **Header and Footer** under the **View** menu. Click on and review both the **Slide** and the **Notes and Handouts** tab.

b. Review the Masters for the file. To do this: Click on **Master** under the **View** menu. Then select and review each of the Masters (Slide, Title, Handout, & Notes).

c. For each slide, click on **Edit**, then **Select All**. Once all objects are selected, click on **Draw** (bottom left of screen), then **Ungroup**, until the Ungroup option is no longer available (grayed out). Hit the tab key to outline each object (delineated by a box around a graphic or text), in the slide. If an object is outlined but not visible, move it, bring it forward or change its color until it is visible, or delete it. Repeat this process for each object in the slide. Use this process to find and delete all higher classified information.

d. After the review is complete, save the information in one of the authorized formats. To do this: Click on **File Save As** under the **File** menu. Select one of the DSS authorized formats from the drop-down menu of **Save As Type**.

6. If any files are not in one of the following five formats, ASCII/Text, HTM/HTML, JPEG, BMP, GIF, convert it to one of these formats.

a. Spreadsheet and database files must be exported as an ASCII text file(s).

b. The graphics files within HTM/HTML files must be saved separately as JPG files. HTML files by themselves are text information and may be treated as a standard ASCII file format.

☐ This page is not applicable

c. Executable programs may not be transferred. The source code (ASCII text) may be reviewed/transferred to a lower level IS then re-compiled into executable code.

7. Review the file(s) using a compatible application. Review the entire file(s) not just random samples.

a. BMP and JPG files may be reviewed with a graphics file viewer such as MS Photo Editor. (Note: because GIF files may contain a 3D/animation/multi-page image, you must use a program that will show all the information stored in GIF files. Internet Explorer or Netscape can be used. MS Photo Editor will not display all the frames (images) and therefore is not adequate to view GIF files).

b. For ASCII text, the preferred application for reviewing is NotePad. However, these applications have file size limitations. If the file may not be opened with NotePad, then use MS Word (step d below).

c. After completion of the review, remove all encoded formatting created by previous editing with MS Word. To do this: On the **File** menu**,** click **Save As…. (Selected Approved Format)** then click **Save**.

d. Review remaining ASCII files not viewable with NotePad with MS Word:

(1) Ensure all hidden text and codes are viewable. To do this: Click **Options** on the **Tools** menu, click the **View** tab, then select every option under the **Show** section and **All** under **the Formatting Marks** section.

(2) Verify all Tracked changes (Revisions in MS Word) are viewable. To do this: Click on **Track Changes** then **Highlight Changes** under the **Tools** menu. If Enabled, Disable the **Track changes while editing**. Enable the **Highlight changes on screen**.

(3) Review the Summary and Contents sections of the file properties. To do this: Click **Properties** on the **File** menu, then click on the **Summary** and **Contents** tabs.

(4) Review Headers and Footers. To do this: Click on **Header and Footer** under the **View** menu. Headers will be displayed at the top of each page, any footers will be displayed at the bottom of each page. Note: If a document has multiple Sections, each Section may have different Headers and Footers.

(5) Review Comments. To do this: Click on **Comments** under the **View** menu. A comments pane will be displayed at the bottom of the screen. If Comments is grayed out under the View menu, this means there are no comments within the document.

(6) Review Footnotes: To do this: Click on **Footnotes** under the **View** menu. If Footnotes is grayed out under the View menu, this means there are no footnotes within the document. If footnotes are not grayed out there are footnotes. If you are displaying the document in Normal layout or Web Layout, a footnote pane will appear at the bottom of the screen. If you are displaying the document in Print Layout, footnotes will already be visible at the bottom of each page, or at the end of the document.

(7) Review the entire contents of the file including all Sections. All embedded objects except clipart and WordArt must be deleted. When reviewing clipart and WordArt and text boxes ensure there is no information hidden behind these objects. Note: Embedded objects may be opened and saved separately prior to deletion. Each separately saved object is subject to this procedure prior to transfer.

(8) When you are finished reviewing the file, ensure all hidden deleted information from Fast Save operations is removed. To do this: On the **File** menu**,** click **Save As …(Selected Approved Format)** then click **Save**. Also, if the file is not yet in one of the acceptable file format types, select one of the DSS approved formats from the drop-down menu of **Save As Type**.

e. For all file formats, verify the source and target file(s) names are not classified.

IS Profile Attachment 9

☐ This page is not applicable

8. Use the standard save or transfer command or utility (i.e. drag and drop, copy, etc) to transfer the file(s) to the target media.

9. Write-protect the media (physical or software) as soon as the transfer(s) are complete.

10. Verify (dir/s [drive]: or Windows Explorer) that only intended file(s) were transferred.

11. Compare the file(s) that were transferred to the original(s) [fc (pathname/filename) drive: (path/ filename)].

12. Apply the appropriate security classification label to the target media.

13. Create an administrative record of the transfer and maintain with your audit records. The record must specify the data being released, the personnel involved and the date.

☐ This page is not applicable

DSS Authorized Procedure (Unix)

Note: These procedures should be tailored for the local environment. In particular, the Unix commands listed herein are for illustration only and must be modified to account for the Unix version, hardware configuration, and software installation specifics.

1. Target media must be new.

2. Procedure must be performed by a "Knowledgeable User".

3. If multiple files are being transferred, create a designated source directory for the transfer using the Unix make directory command (mkdir directory_name). Rationale: This will establish an empty directory. This two-step process helps ensure that only intended files are copied.

4. If multiple files are being transferred, transfer all files into the newly created directory.

5. Verify the source and target file(s) names are not classified.

6. View the contents of all file(s) in the designated directory, not just "random samples."

   a. For text files use software that displays the entire contents of the file. (EG: Hex editor) Any unintelligible data is assumed to be classified at the accredited IS level.

   b. For graphics or movie files review the file(s) using an appropriate file viewer. Ensure that the file format does not include internal annotations or other additional data (if present, this information can only be viewed with a specialized viewer, and poses a significant threat of inadvertent disclosure).

   c. For non-text files the sensitivity or classification of non-text, non-graphics files cannot generally be determined without intensive technical analysis. Such files must be assumed to be classified. Files in this category include binary database files, compressed archives, and executable code.

      (1) In the case of executable files, review and downgrade the source code, then transfer the source code to a lower-classified machine for re-compilation.

      (2) In some cases, the source code will be classified, but the compiled code will be unclassified as specified in the classification guidance document. After compilation, the executable must be reviewed with HEX editor software to ensure that no classified information has escaped the compilation process.

      (3) In the case of binary database files, export the data to ASCII text format, then review and downgrade the text file for media migration.

      (4) Compressed archives should be reviewed and transferred uncompressed.

7. Use the Tar utility to create and write an archive of the source directory to the target media. The Unix command sequence will be as shown below (the exact command may vary depending on the Unix version, machine configuration, and the media used):

   mt -f /dev/rst0 rew Ensure tape is rewound (not required if using floppy)

   tar cvf /dev/rst0 /directory_name Create Tar file on tape

8. Write-protect the media as soon as the transfer(s) are complete.

IS Profile Attachment 9

☐ This page is not applicable

9. Verify that the media contains the expected data by printing a directory of the Tar file:

mt -f /dev/rst0 rew Ensure tape is rewound (not required for floppy)

tar tvf /dev/rst0 | lpr Print directory of file (| lpr may be omitted for on-screen review)

10. The output of the above command should match the contents of the source directory. To verify that they match, compare the output of the above command with the directory printed by the following command:

ls -alR /source-directory | lpr (| lpr may be omitted for on-screen review)

11. Ensure the date, time, and file size(s) are as expected. If any unintended data was copied, the target media must be considered classified and cannot be used for a trusted down load again.

12. Apply the appropriate security classification label to the target media.

13. Create an administrative record of the transfer and maintain with your audit records. The record must specify the data being released, the personnel involved and the date.

☐ This page is not applicable

Trusted Download Authorization

Printed Name:	Job Function or Title:

Manager Request	
I request the above named individual be authorized to perform trusted downloads. I understand this access requires training to perform trusted downloads, a process for generating unclassified or lower classified media from a classified system. I understand this process involves both knowledge of classification issues and attention to detail in reviewing information and following the process for performing a download. I also understand that transferring information from a classified environment to an unclassified environment increases the risk of compromising classified information and will instruct authorized employees under my supervision to perform these actions only when absolutely necessary.	
Printed Name:	
Signature:	Date:

Acceptance of Responsibility	
I have attended a trusted download training class and understand both the risks associated with performing a Trusted Download and the mechanisms associated with the trusted download process. I understand that all media generated from a classified system must be labeled and handled at the highest level of data on the system unless a trusted download procedure is performed. I understand it is my responsibility to perform this process as outlined in the trusted download procedure.	
Signature:	Date:

ISSM or ISSO Authorization	
I certify that the individual identified above has been briefed in the vulnerabilities associated with transferring unclassified or lower classified information from an accredited information system (i.e., trusted download). Additionally, he/she has demonstrated extensive knowledge of all appropriate security classification guide(s) and authorized procedures associated with the information downloaded.	
Authorized File Formats: ASCII/Text, HTM/HTML, JPEG, BMP, GIF Specify:	
Printed Name:	
Signature:	Date:

IS Profile Attachment 9

☐ This page is not applicable

Trusted Download Record

Date	Person	File Type	File Description

IS Profile Attachment 9

Operating System(s):	Version(s):

Accounts, Logons, and Session Controls

Identification & Authentication (I&A) is technically enforced: ☐ Yes ☐ No If No, Users will manually record User Access, Refer to Attachment:

Password generation routine: ☐ IS generated random password ☐ Passwords assigned by administrator ☐ User generated passwords
Check if Technically Enforceable: ☐ Password Length ☐ Password Complexity
Password lifetime (# of days):

Periods processing: ☐ No ☐ Yes* (Explain procedures in addl info/comments section at end of document.)

Lockouts for multiple failed logins: ☐ Yes, After attempts and ☐ After minutes and\or ☐ an administrator is required to unlock the account.

I&A Management: Describe how User IDs & Passwords are established and distributed:

User Accounts will be validated annually by: ☐ System Administrator ☐ ISSM ☐ ISSO ☐ Other, Specify:

Generic or Group accounts: ☐ No ☐ Yes* If yes, list each group account (group authorization) on IS, with a justification for their use:

Account Name: Justification:

Account Name: Justification:

Account Name: Justification:

*When group accounts are used, manual logs (or other methods) should be utilized to assure individual accountability.

System Audit Capabilities

Automated Audit Trails: ☐ No ☐ Yes If yes, Identify Audit Mechanism:	**Audit Capabilities -** Check all that are technically feasible and enabled: ☐ Successful Logons ☐ Unsuccessful logons ☐ Logoffs ☐ Denial of System access due to failed logins ☐ Unsuccessful access to objects ☐ Changes in Passwords

Audit Management:
Automated audit records are maintained: ☐ Locally to each system ☐ Offline via media
Audit overflow configuration ☐ System will shutdown
Retention period for online audit records: Retention period for offline audit records:

Description of IS Records and Logs:
In addition to the automated logs generated by the system, records and logs of IS
☐ Records and logs are generated and maintained manually in hardcopy form, examples are attached
☐ Some IS changes or actions are recorded within online automated systems. Describe:

Virus and Malicious Code Detection	Access Controls to Security Relevant Objects
Virus Detection Software Installed: ☐ Yes ☐ No If yes, how often are signature files updated: If No, Alternate method:	This IS is capable of file permissions or ACLs: ☐ Yes ☐ No

ISSM System Certification Test Checklist	
Facility Name:	**IS#:**

Reference: Certification testing and ongoing security testing are the verification of correct operation of the protection measures in a system. In accordance with NISPOM 8-103g, 8-201, 8-610a2 and 8-614a, the ISSM will perform and document that the system operates in accordance with the approved SSP and that the security features, including access controls and configuration management, are implemented and operational.

	N/A	S	F
Physical Area Safeguards			
Closed Area: verify the area has been approved and all Closed Area procedures and mechanisms are in place. (NISPOM 8-308)	☐	☐	☐
Restricted area: verify components are positioned so that classified information displayed or output during processing will not be visible to unauthorized persons. Verify all required locks, seals, or barriers are in place. (NISPOM 8-308)	☐	☐	☐
All areas: Verify all IS components in the hardware baseline reside in the IS controlled area.	☐	☐	☐
Verify a container approved for storage of classified materials or classified waste is available for use.	☐	☐	☐
Authorized Users/Training			
Verify the clearance, Need-to-Know, and any additional accesses (if applicable) for each IS User. (NISPOM 8-303 and 8-309)	☐	☐	☐
If applicable, verify that visitors, subcontractors and consultants have JPAS eligibility or a current Visit Authorization letter on file with your facility. (NISPOM 8-606a).	☐	☐	☐
Verify each IS user has received initial training regarding their IS responsibilities and has signed a User Authorization form. (NISPOM 3-106e and 8-307)	☐	☐	☐
Hardware Configuration			
Verify the IS hardware components match the IS Profile Hardware baseline. (NISPOM 8-610a(1)(d))	☐	☐	☐
Verify the configuration of the IS is compliant with the Configuration Diagram contained in the Profile and that all hardware and connections are listed. (NISPOM 8-610a1d)	☐	☐	☐
Verify all IS hardware has been examined to determine that it is in good working order. (NISPOM 8-302b)	☐	☐	☐
Software Configuration and Media			
Verify the software resident on the system is in accordance with the Software Baseline in the Profile.(NISPOM 8-610)	☐	☐	☐
Verify there is a backup protected copy of all software dedicated to classified processing sessions. (NISPOM 8-304b(4))	☐	☐	☐
Verify all classified media has all appropriate NISPOM required markings. (NISPOM 8-306)	☐	☐	☐
Top secret: If applicable, verify Top Secret media has been placed into accountability. (NISPOM 5-203)	☐	☐	☐
Co-located: If there are co-located systems dedicated to unclassified processing in the IS controlled area, verify all unclassified media is marked as Unclassified. (NISPOM 8-306c)	☐	☐	☐
Verify media dedicated to maintenance activities is labeled “Unclassified – For Maintenance Only” (NISPOM 8-304b(4))	☐	☐	☐
Labeling			
Verify all hardware that will retain information when power is removed has a conspicuous external classification label. (NISPOM 8-306a)	☐	☐	☐
Verify all systems or workstations that are co-located in the area, but are not part of the accredited IS baseline have been conspicuously labeled to indicate their use is limited to unclassified processing. (NISPOM 8-306a)	☐	☐	☐

IS Profile Attachment 10

ISSM System Certification Test Checklist	
Facility Name:	**IS#:**

Instructions: Most protection measures on this page are implemented through IS technical controls. This portion of the certification test guide must be filled out for each platform contained on the system (e.g. Windows 2000, Sun Solaris 8.0). Verify all technical controls are in place and operating correctly. **S** denotes the results for a particular technical control are in place and operating successfully. **F** denotes the technical control is not in place or the verification test failed**. All failed results must have a corrective action taken prior to certifying the IS.** Specify **N/A** if the particular technical control does not apply to this IS (for example, a single user standalone does not require technical audit controls and verification may be N/A).

Profile Version#:	**Operating System:**	**O/S Version #:**

	N/A	S	F
Logon Authentication			
Technical Implementation: If logon authentication is technically implemented, verify that IS users are required to present their User ID and authenticator to gain access (NISPOM 8-303)	☐	☐	☐
If user access is not technically implemented through logon authentication (single user standalones), verify physical security controls and personnel security controls such as an Authorized User List are sufficient. (NISPOM 8-303c)	☐	☐	☐
Session Controls			
Technical Implementation: Verify the DSS or contractually required logon banner is displayed on all systems and that the user is required to take positive action to remove the notice from the screen. (NISPOM 8-609a(1))	☐	☐	☐
If the warning banner is not technically implemented, verify it is prominently displayed in the area or other methods of notification are developed and approved by DSS. (NISPOM 8-609a(1)).	☐	☐	☐
If the OS is capable, verify that successive logon attempts are controlled by: denying access after multiple consecutive unsuccessful access attempts of the same user ID, limiting number of access attempts within a time period, by use of a time delay control. (NISPOM 8-609(2))	☐	☐	☐
Verify system entry granted only in accordance with user's profile and if not explicitly granted, verify all remote activities such as remote logons and anonymous file accesses are prohibited. (NISPOM 8-609(3))	☐	☐	☐
Password Controls			
Verify that when passwords are entered they are not visible (must be masked). (NISPOM 8-303i(4))	☐	☐	☐
Password Generation: If the IS generates the passwords, verify the IS generates a random password that is a minimum of 14 non-blank characters. (NISPOM 8-303i(2))	☐	☐	☐
If passwords are User generated, verify the following features, as specified in the profile, are properly functioning: Minimum password length (14-characters), Password composition (mixture of characters/numbers, and upper/lower case) Capability to require a password change upon reaching the allowed password lifetime. (NISPOM 8-303i)	☐	☐	☐
If present, verify that vendor standard accounts with pre-defined passwords have been changed or disabled. Verify that they have also been changed or disabled after a new system version is installed or other action initiated that might result in restoration of these passwords/accounts. (NISPOM 8-303i(5))	☐	☐	☐
Group Accounts: If group authenticators are used, verify they are used in association with individual authenticators. (NISPOM 8-607b and 8-505)	☐	☐	☐
If present, verify that the BIOS setup, EEPROM access or single user mode, GRUB or LILO loader is password protected. (NISPOM 8-613a(1))	☐	☐	☐
Access Protections			
Verify that the file(s) containing passwords is either not accessible to non-privileged users, or that the passwords are encrypted. (NISPOM 8-303d)	☐	☐	☐
Verify that the file(s) containing audit data is not accessible to non-privileged users. (NISPOM 8-602a(2))	☐	☐	☐

Verify the files and directories that control the system and/or its security may not be modified or deleted by non-privileged users. (NISPOM 8-613)	☐	☐	☐
Verify that writing to floppy drives, CD-ROM drives, or use of USB drives, not expressly permitted by the security policy are prohibited. (NISPOM 8-609a(3) and 8-606)	☐	☐	☐
Verify that security procedures are in place to mitigate risks inherent with wireless devices. (NISPOM 1-200 and ISL 2006-02, Q1)	☐	☐	☐
Audit Mechanisms			
Verify that systems capable of audit have auditing enabled or if the system is incapable of audit, the GCA has provided contract documentation that clearly directs the use of those operating systems. (NISPOM 8-602, ISL 2007-01, Q41)	☐	☐	☐
Verify the system is recording successful and unsuccessful logons and logoffs. (NISPOM 8-602a(1)(b))	☐	☐	☐
Verify the system is recording unsuccessful attempts to access security relevant files and directories. (NISPOM 8-602a(1)(c))	☐	☐	☐
Verify the system is recording denial of system access (account lockout) due to multiple failed login attempts. (NISPOM 8-602a(1)(f))	☐	☐	☐
Verify the system is recording changes to passwords. (NISPOM 8-602a(1)(d))	☐	☐	☐
Verify that the audit records generated by the system contain the following information: date and time of the action, type of action, and the responsible person for the action, and the resources involved (e.g. name of file for a failed access attempt of a file). (NISPOM 8-602a(1)(a))	☐	☐	☐
Virus Detection and Malicious Code			
Verify that virus detection software has been installed, is functional, and has been executed on all installed media. (NISPOM 8-305)	☐	☐	☐
Verify that all IS software has been tested for malicious code as feasible. (NISPOM 8-305)	☐	☐	☐
Sanitization Procedures			
Verify all sanitization procedures have been validated. (NISPOM 8-301 and DSS Clearing and Sanitization Matrix)	☐	☐	☐
Trusted Download Procedure			
Verify that trusted download procedures are in accordance with DSS procedures and formats or that the GCA has acknowledged the Risk via DD254, contract, or memorandum. (NISPOM 8-310b)	☐	☐	☐
Networks			
Transmission: Verify transmission is through a Protected Distribution System or by use of an NSA Type 1 Encryptor. (NSTISSI 7003)	☐	☐	☐
Interconnected network: Verify security policy is in accordance with the DSS Approved Network Security Plan. (NISPOM 8-700)	☐	☐	☐
Interconnected network: If connected to a government system, verify security policy is in accordance with MOU. (NISPOM 8-700)	☐	☐	☐

Letter Acknowledging Relocation of IS By Contractor Site (Sample)

CONTRACTOR LETTERHEAD

(To be used when releasing IS to Government or test site for over one week.)

(DATE)

FROM: (ISSM)

TO: (Name of Government site POC and address)

SUBJECT: Relocation of DSS Accredited Information System (number) from (Company Name) to (Government Site).

1. On (Accreditation Date) the Defense Security Service (DSS) accredited under the National Industrial Security Program Operating Manual (NISPOM) information system (IS) (Name or number of IS) located at (Company Name) to process classified information at the (Level of Information) level. A copy of the accreditation letter is attached for your review.

2. (Company name) has a requirement in conjunction with (Contract number) with (Name of GCA) to relocate the above to (Name of Government site) in order to process classified information for (Purpose). During the period when this will be resident at (Name of Government site, test site, or installation, etc.) your activity must assume cognizance for the security of the system. Any movement of an accredited IS outside of the DSS-approved area changes the original intent of DSS' accreditation. As you are aware, different risks and vulnerabilities are associated with moving an IS, to include, for example, different threats to the IS or classified information, different physical security factors and different user need-to-know concerns.

3. Prior to the above system being relocated to your site, an authorized official of (Name of site) must sign this letter [where indicated below] and return it to the address provided. Your authorized official's signature will represent your organization's formal concurrence to accept security cognizance for the above-specified IS while it will be located at your site and under your jurisdiction. (Name of Contractor) anticipates the IS (or Closed Area) will be removed from (Name of site), and consequently your jurisdiction, by (provide approximate time of removal and location to which the system will be subsequently relocated).

4. If you have questions or would like to discuss this, please contact (Company POC) at (telephone number) or by email at (email).

Sincerely,

(ISSM's Name)
(Title/Company)

Attachments: DSS Accreditation Letter
Dated (Date)

Copy to: (Cognizant DSS ISR)

CONCURRENCE:

(Name/Title of Authorized Official)

☒ This page is not applicable

Operating System(s):	**Version(s):**

Accounts, Logons, and Session Controls

Identification & Authentication (I&A) is technically enforced: ☐ Yes ☐ No If No, Users will manually record User Access, Refer to Attachment:

Password generation routine: ☐ IS generated random password ☐ Passwords assigned by administrator ☐ User generated passwords

Check if Technically Enforceable: ☐ Password Length ☐ Password Complexity

Password lifetime (# of days):

Periods processing: ☐ No ☐ Yes* (Explain procedures in addl info/comments section at end of document.)

Lockouts for multiple failed logins: ☐ Yes, After attempts and ☐ After minutes and\or ☐ an administrator is required to unlock the account.

I&A Management: Describe how User IDs & Passwords are established and distributed:

User Accounts will be validated annually by: ☐ System Administrator ☐ ISSM ☐ ISSO ☐ Other, Specify:

Generic or Group accounts: ☐ No ☐ Yes* If yes, list each group account (group authorization) on IS, with a justification for their use:

Account Name: Justification:

Account Name: Justification:

Account Name: Justification:

*When group accounts are used, manual logs (or other methods) should be utilized to assure individual accountability.

System Audit Capabilities

Automated Audit Trails: ☐ No ☐ Yes If yes, Identify Audit Mechanism:	**Audit Capabilities -** Check all that are technically feasible and enabled: ☐ Successful Logons ☐ Unsuccessful logons ☐ Logoffs ☐ Denial of System access due to failed logins ☐ Unsuccessful access to objects ☐ Changes in Passwords

Audit Management:

Automated audit records are maintained: ☐ Locally to each system ☐ Offline via media

Audit overflow configuration: ☐ System will shutdown

Retention period for online audit records: Retention period for offline audit records:

Description of IS Records and Logs:

In addition to the automated logs generated by the system, records and logs of IS

☐ All records and logs are generated and maintained manually in hardcopy form, examples are attached

☐ Some IS changes or actions are recorded within online automated systems. Describe:

Virus and Malicious Code Detection	**Access Controls to Security Relevant Objects**
Virus Detection Software Installed: ☐ Yes ☐ No If yes, how often are signature files updated: If No, Alternate method:	This IS is capable of file permissions or ACLs: ☐ Yes ☐ No

☒ This page is not applicable

ISSM System Certification Test Checklist	
Facility Name:	**IS#:**

Instructions: Most protection measures on this page are implemented through IS technical controls. This portion of the certification test guide must be filled out for each platform contained on the system (e.g. Windows 2000, Sun Solaris 8.0). Verify all technical controls are in place and operating correctly. **S** denotes the results for a particular technical control are in place and operating successfully. **F** denotes the technical control is not in place or the verification test failed**. All failed results must have a corrective action taken prior to certifying the IS.** Specify **N/A** if the particular technical control does not apply to this IS (for example, a single user standalone does not require technical audit controls and verification may be N/A).

Profile Version#:	**Operating System:**	**O/S Version #:**

	N/A	S	F
Logon Authentication			
Technical Implementation: If logon authentication is technically implemented, verify that IS users are required to present their User ID and authenticator to gain access (NISPOM 8-303)	☐	☐	☐
If user access is not technically implemented through logon authentication (single user standalones), verify physical security controls and personnel security controls such as an Authorized User List are sufficient. (NISPOM 8-303c)	☐	☐	☐
Session Controls			
Technical Implementation: Verify the DSS or contractually required logon banner is displayed on all systems and that the user is required to take positive action to remove the notice from the screen. (NISPOM 8-609a(1))	☐	☐	☐
If the warning banner is not technically implemented, verify it is prominently displayed in the area or other methods of notification are developed and approved by DSS. (NISPOM 8-609a(1)).	☐	☐	☐
If the OS is capable, verify that successive logon attempts are controlled by: denying access after multiple consecutive unsuccessful access attempts of the same user ID, limiting number of access attempts within a time period, by use of a time delay control. (NISPOM 8-609(2))	☐	☐	☐
Verify system entry granted only in accordance with user's profile and if not explicitly granted, verify all remote activities such as remote logons and anonymous file accesses are prohibited. (NISPOM 8-609(3))	☐	☐	☐
Password Controls			
Verify that when passwords are entered they are not visible (must be masked). (NISPOM 8-303i(4))	☐	☐	☐
Password Generation: If the IS generates the passwords, verify the IS generates a random password that is a minimum of 14 non-blank characters. (NISPOM 8-303i(2))	☐	☐	☐
If passwords are User generated, verify the following features, as specified in the profile, are properly functioning: Minimum password length (14-characters), Password composition (mixture of characters/numbers, and upper/lower case) Capability to require a password change upon reaching the allowed password lifetime. (NISPOM 8-303i)	☐	☐	☐
If present, verify that vendor standard accounts with pre-defined passwords have been changed or disabled. Verify that they have also been changed or disabled after a new system version is installed or other action initiated that might result in restoration of these passwords/accounts. (NISPOM 8-303i(5))	☐	☐	☐
Group Accounts: If group authenticators are used, verify they are used in association with individual authenticators. (NISPOM 8-607b and 8-505)	☐	☐	☐
If present, verify that the BIOS setup, EEPROM access or single user mode, GRUB or LILO loader is password protected. (NISPOM 8-613a(1))	☐	☐	☐
Access Protections			
Verify that the file(s) containing passwords is either not accessible to non-privileged users, or that the passwords are encrypted. (NISPOM 8-303d)	☐	☐	☐
Verify that the file(s) containing audit data is not accessible to non-privileged users. (NISPOM 8-602a(2))	☐	☐	☐

☒ This page is not applicable

Verify the files and directories that control the system and/or its security may not be modified or deleted by non-privileged users. (NISPOM 8-613)	☐	☐	☐
Verify that writing to floppy drives, CD-ROM drives, or use of USB drives, not expressly permitted by the security policy are prohibited. (NISPOM 8-609a(3) and 8-606)	☐	☐	☐
Verify that security procedures are in place to mitigate risks inherent with wireless devices. (NISPOM 1-200 and ISL 2006-02, Q1)	☐	☐	☐
Audit Mechanisms			
Verify that systems capable of audit have auditing enabled or if the system is incapable of audit, the GCA has provided contract documentation that clearly directs the use of those operating systems. (NISPOM 8-602, ISL 2007-01, Q41)	☐	☐	☐
Verify the system is recording successful and unsuccessful logons and logoffs. (NISPOM 8-602a(1)(b))	☐	☐	☐
Verify the system is recording unsuccessful attempts to access security relevant files and directories. (NISPOM 8-602a(1)(c))	☐	☐	☐
Verify the system is recording denial of system access (account lockout) due to multiple failed login attempts. (NISPOM 8-602a(1)(f))	☐	☐	☐
Verify the system is recording changes to passwords. (NISPOM 8-602a(1)(d))	☐	☐	☐
Verify that the audit records generated by the system contain the following information: date and time of the action, type of action, and the responsible person for the action, and the resources involved (e.g. name of file for a failed access attempt of a file). (NISPOM 8-602a(1)(a))	☐	☐	☐
Virus Detection and Malicious Code			
Verify that virus detection software has been installed, is functional, and has been executed on all installed media. (NISPOM 8-305)	☐	☐	☐
Verify that all IS software has been tested for malicious code as feasible. (NISPOM 8-305)	☐	☐	☐
Sanitization Procedures			
Verify all sanitization procedures have been validated. (NISPOM 8-301 and DSS Clearing and Sanitization Matrix)	☐	☐	☐
	☐	☐	☐
Trusted Download Procedure			
Verify that trusted download procedures are in accordance with DSS procedures and formats or that the GCA has acknowledged the Risk via DD254, contract, or memorandum. (NISPOM 8-310b)	☐	☐	☐
Networks			
Transmission: Verify transmission is through a Protected Distribution System or by use of an NSA Type 1 Encryptor. (NSTISSI 7003)	☐	☐	☐
Interconnected network: Verify security policy is in accordance with the DSS Approved Network Security Plan. (NISPOM 8-700)	☐	☐	☐
Interconnected network: If connected to a government system, verify security policy is in accordance with MOU. (NISPOM 8-700)	☐	☐	☐

☒ This page is not applicable

Operating System(s):	**Version(s):**

Accounts, Logons, and Session Controls

Identification & Authentication (I&A) is technically enforced: ☐ Yes ☐ No If No, Users will manually record User Access, Refer to Attachment:

Password generation routine: ☐ IS generated random password ☐ Passwords assigned by administrator ☐ User generated passwords

Check if Technically Enforceable: ☐ Password Length ☐ Password Complexity

Password lifetime (# of days):

Periods processing: ☐ No ☐ Yes* (Explain procedures in addl info/comments section at end of document.)

Lockouts for multiple failed logins: ☐ Yes, After attempts and ☐ After minutes and\or ☐ an administrator is required to unlock the account.

I&A Management: Describe how User IDs & Passwords are established and distributed:

User Accounts will be validated annually by: ☐ System Administrator ☐ ISSM ☐ ISSO ☐ Other, Specify:

Generic or Group accounts: ☐ No ☐ Yes* If yes, list each group account (group authorization) on IS, with a justification for their use:

Account Name: Justification:

Account Name: Justification:

Account Name: Justification:

*When group accounts are used, manual logs (or other methods) should be utilized to assure individual accountability.

System Audit Capabilities

Automated Audit Trails: ☐ No ☐ Yes If yes, Identify Audit Mechanism:	**Audit Capabilities -** Check all that are technically feasible and enabled: ☐ Successful Logons ☐ Unsuccessful logons ☐ Logoffs ☐ Denial of System access due to failed logins ☐ Unsuccessful access to objects ☐ Changes in Passwords

Audit Management:

Automated audit records are maintained: ☐ Locally to each system ☐ Offline via media

Audit overflow configuration: ☐ System will shutdown

Retention period for online audit records: Retention period for offline audit records:

Description of IS Records and Logs:

In addition to the automated logs generated by the system, records and logs of IS

☐ All records and logs are generated and maintained manually in hardcopy form, examples are attached

☐ Some IS changes or actions are recorded within online automated systems. Describe:

Virus and Malicious Code Detection	**Access Controls to Security Relevant Objects**
Virus Detection Software Installed: ☐ Yes ☐ No If yes, how often are signature files updated: If No, Alternate method:	This IS is capable of file permissions or ACLs: ☐ Yes ☐ No

☒ This page is not applicable

ISSM System Certification Test Checklist	
Facility Name:	**IS#:**

Instructions: Most protection measures on this page are implemented through IS technical controls. This portion of the certification test guide must be filled out for each platform contained on the system (e.g. Windows 2000, Sun Solaris 8.0). Verify all technical controls are in place and operating correctly. **S** denotes the results for a particular technical control are in place and operating successfully. **F** denotes the technical control is not in place or the verification test failed**. All failed results must have a corrective action taken prior to certifying the IS.** Specify **N/A** if the particular technical control does not apply to this IS (for example, a single user standalone does not require technical audit controls and verification may be N/A).

Profile Version#:	**Operating System:**	**O/S Version #:**

	N/A	S	F
Logon Authentication			
Technical Implementation: If logon authentication is technically implemented, verify that IS users are required to present their User ID and authenticator to gain access (NISPOM 8-303)	☐	☐	☐
If user access is not technically implemented through logon authentication (single user standalones), verify physical security controls and personnel security controls such as an Authorized User List are sufficient. (NISPOM 8-303c)	☐	☐	☐
Session Controls			
Technical Implementation: Verify the DSS or contractually required logon banner is displayed on all systems and that the user is required to take positive action to remove the notice from the screen. (NISPOM 8-609a(1))	☐	☐	☐
If the warning banner is not technically implemented, verify it is prominently displayed in the area or other methods of notification are developed and approved by DSS. (NISPOM 8-609a(1)).	☐	☐	☐
If the OS is capable, verify that successive logon attempts are controlled by: denying access after multiple consecutive unsuccessful access attempts of the same user ID, limiting number of access attempts within a time period, by use of a time delay control. (NISPOM 8-609(2))	☐	☐	☐
Verify system entry granted only in accordance with user's profile and if not explicitly granted, verify all remote activities such as remote logons and anonymous file accesses are prohibited. (NISPOM 8-609(3))	☐	☐	☐
Password Controls			
Verify that when passwords are entered they are not visible (must be masked). (NISPOM 8-303i(4))	☐	☐	☐
Password Generation: If the IS generates the passwords, verify the IS generates a random password that is a minimum of 14 non-blank characters. (NISPOM 8-303i(2))	☐	☐	☐
If passwords are User generated, verify the following features, as specified in the profile, are properly functioning: Minimum password length (14-characters), Password composition (mixture of characters/numbers, and upper/lower case) Capability to require a password change upon reaching the allowed password lifetime. (NISPOM 8-303i)	☐	☐	☐
If present, verify that vendor standard accounts with pre-defined passwords have been changed or disabled. Verify that they have also been changed or disabled after a new system version is installed or other action initiated that might result in restoration of these passwords/accounts. (NISPOM 8-303i(5))	☐	☐	☐
Group Accounts: If group authenticators are used, verify they are used in association with individual authenticators. (NISPOM 8-607b and 8-505)	☐	☐	☐
If present, verify that the BIOS setup, EEPROM access or single user mode, GRUB or LILO loader is password protected. (NISPOM 8-613a(1))	☐	☐	☐
Access Protections			
Verify that the file(s) containing passwords is either not accessible to non-privileged users, or that the passwords are encrypted. (NISPOM 8-303d)	☐	☐	☐
Verify that the file(s) containing audit data is not accessible to non-privileged users. (NISPOM 8-602a(2))	☐	☐	☐

☒ This page is not applicable

Verify the files and directories that control the system and/or its security may not be modified or deleted by non-privileged users. (NISPOM 8-613)	☐	☐	☐
Verify that writing to floppy drives, CD-ROM drives, or use of USB drives, not expressly permitted by the security policy are prohibited. (NISPOM 8-609a(3) and 8-606)	☐	☐	☐
Verify that security procedures are in place to mitigate risks inherent with wireless devices. (NISPOM 1-200 and ISL 2006-02, Q1)	☐	☐	☐
Audit Mechanisms			
Verify that systems capable of audit have auditing enabled or if the system is incapable of audit, the GCA has provided contract documentation that clearly directs the use of those operating systems. (NISPOM 8-602, ISL 2007-01, Q41)	☐	☐	☐
Verify the system is recording successful and unsuccessful logons and logoffs. (NISPOM 8-602a(1)(b))	☐	☐	☐
Verify the system is recording unsuccessful attempts to access security relevant files and directories. (NISPOM 8-602a(1)(c))	☐	☐	☐
Verify the system is recording denial of system access (account lockout) due to multiple failed login attempts. (NISPOM 8-602a(1)(f))	☐	☐	☐
Verify the system is recording changes to passwords. (NISPOM 8-602a(1)(d))	☐	☐	☐
Verify that the audit records generated by the system contain the following information: date and time of the action, type of action, and the responsible person for the action, and the resources involved (e.g. name of file for a failed access attempt of a file). (NISPOM 8-602a(1)(a))	☐	☐	☐
Virus Detection and Malicious Code			
Verify that virus detection software has been installed, is functional, and has been executed on all installed media. (NISPOM 8-305)	☐	☐	☐
Verify that all IS software has been tested for malicious code as feasible. (NISPOM 8-305)	☐	☐	☐
Sanitization Procedures			
Verify all sanitization procedures have been validated. (NISPOM 8-301 and DSS Clearing and Sanitization Matrix)	☐	☐	☐
Trusted Download Procedure			
Verify that trusted download procedures are in accordance with DSS procedures and formats or that the GCA has acknowledged the Risk via DD254, contract, or memorandum. (NISPOM 8-310b)	☐	☐	☐
Networks			
Transmission: Verify transmission is through a Protected Distribution System or by use of an NSA Type 1 Encryptor. (NSTISSI 7003)	☐	☐	☐
Interconnected network: Verify security policy is in accordance with the DSS Approved Network Security Plan. (NISPOM 8-700)	☐	☐	☐
Interconnected network: If connected to a government system, verify security policy is in accordance with MOU. (NISPOM 8-700)	☐	☐	☐

☒ This page is not applicable

Operating System(s):	**Version(s):**

Accounts, Logons, and Session Controls

Identification & Authentication (I&A) is technically enforced: ☐ Yes ☐ No If No, Users will manually record User Access, Refer to Attachment:

Password generation routine: ☐ IS generated random password ☐ Passwords assigned by administrator ☐ User generated passwords

Check if Technically Enforceable: ☐ Password Length ☐ Password Complexity

Password lifetime (# of days):

Periods processing: ☐ No ☐ Yes* (Explain procedures in addl info/comments section at end of document.)

Lockouts for multiple failed logins: ☐ Yes, After attempts and ☐ After minutes and\or ☐ an administrator is required to unlock the account.

I&A Management: Describe how User IDs & Passwords are established and distributed:

User Accounts will be validated annually by: ☐ System Administrator ☐ ISSM ☐ ISSO ☐ Other, Specify:

Generic or Group accounts: ☐ No ☐ Yes* If yes, list each group account (group authorization) on IS, with a justification for their use:

Account Name: Justification:

Account Name: Justification:

Account Name: Justification:

*When group accounts are used, manual logs (or other methods) should be utilized to assure individual accountability.

System Audit Capabilities

Automated Audit Trails: ☐ No ☐ Yes If yes, Identify Audit Mechanism:	**Audit Capabilities -** Check all that are technically feasible and enabled: ☐ Successful Logons ☐ Unsuccessful logons ☐ Logoffs ☐ Denial of System access due to failed logins ☐ Unsuccessful access to objects ☐ Changes in Passwords

Audit Management:

Automated audit records are maintained: ☐ Locally to each system ☐ Offline via media

Audit overflow configuration: ☐ System will shutdown

Retention period for online audit records: Retention period for offline audit records:

Description of IS Records and Logs:

In addition to the automated logs generated by the system, records and logs of IS

☐ All records and logs are generated and maintained manually in hardcopy form, examples are attached

☐ Some IS changes or actions are recorded within online automated systems. Describe:

Virus and Malicious Code Detection	**Access Controls to Security Relevant Objects**
Virus Detection Software Installed: ☐ Yes ☐ No If yes, how often are signature files updated: If No, Alternate method:	This IS is capable of file permissions or ACLs: ☐ Yes ☐ No

☒ This page is not applicable

ISSM System Certification Test Checklist	
Facility Name:	**IS#:**

Instructions: Most protection measures on this page are implemented through IS technical controls. This portion of the certification test guide must be filled out for each platform contained on the system (e.g. Windows 2000, Sun Solaris 8.0). Verify all technical controls are in place and operating correctly. **S** denotes the results for a particular technical control are in place and operating successfully. **F** denotes the technical control is not in place or the verification test failed**. All failed results must have a corrective action taken prior to certifying the IS.** Specify **N/A** if the particular technical control does not apply to this IS (for example, a single user standalone does not require technical audit controls and verification may be N/A).

Profile Version#:	**Operating System:**	**O/S Version #:**

	N/A	S	F
Logon Authentication			
Technical Implementation: If logon authentication is technically implemented, verify that IS users are required to present their User ID and authenticator to gain access (NISPOM 8-303)	☐	☐	☐
If user access is not technically implemented through logon authentication (single user standalones), verify physical security controls and personnel security controls such as an Authorized User List are sufficient. (NISPOM 8-303c)	☐	☐	☐
Session Controls			
Technical Implementation: Verify the DSS or contractually required logon banner is displayed on all systems and that the user is required to take positive action to remove the notice from the screen. (NISPOM 8-609a(1))	☐	☐	☐
If the warning banner is not technically implemented, verify it is prominently displayed in the area or other methods of notification are developed and approved by DSS. (NISPOM 8-609a(1)).	☐	☐	☐
If the OS is capable, verify that successive logon attempts are controlled by: denying access after multiple consecutive unsuccessful access attempts of the same user ID, limiting number of access attempts within a time period, by use of a time delay control. (NISPOM 8-609(2))	☐	☐	☐
Verify system entry granted only in accordance with user's profile and if not explicitly granted, verify all remote activities such as remote logons and anonymous file accesses are prohibited. (NISPOM 8-609(3))	☐	☐	☐
Password Controls			
Verify that when passwords are entered they are not visible (must be masked). (NISPOM 8-303i(4))	☐	☐	☐
Password Generation: If the IS generates the passwords, verify the IS generates a random password that is a minimum of 14 non-blank characters. (NISPOM 8-303i(2))	☐	☐	☐
If passwords are User generated, verify the following features, as specified in the profile, are properly functioning: Minimum password length (14-characters), Password composition (mixture of characters/numbers, and upper/lower case) Capability to require a password change upon reaching the allowed password lifetime. (NISPOM 8-303i)	☐	☐	☐
If present, verify that vendor standard accounts with pre-defined passwords have been changed or disabled. Verify that they have also been changed or disabled after a new system version is installed or other action initiated that might result in restoration of these passwords/accounts. (NISPOM 8-303i(5))	☐	☐	☐
Group Accounts: If group authenticators are used, verify they are used in association with individual authenticators. (NISPOM 8-607b and 8-505)	☐	☐	☐
If present, verify that the BIOS setup, EEPROM access or single user mode, GRUB or LILO loader is password protected. (NISPOM 8-613a(1))	☐	☐	☐
Access Protections			
Verify that the file(s) containing passwords is either not accessible to non-privileged users, or that the passwords are encrypted. (NISPOM 8-303d)	☐	☐	☐
Verify that the file(s) containing audit data is not accessible to non-privileged users. (NISPOM 8-602a(2))	☐	☐	☐

☒ This page is not applicable

Verify the files and directories that control the system and/or its security may not be modified or deleted by non-privileged users. (NISPOM 8-613)	☐	☐	☐
Verify that writing to floppy drives, CD-ROM drives, or use of USB drives, not expressly permitted by the security policy are prohibited. (NISPOM 8-609a(3) and 8-606)	☐	☐	☐
Verify that security procedures are in place to mitigate risks inherent with wireless devices. (NISPOM 1-200 and ISL 2006-02, Q1)	☐	☐	☐
Audit Mechanisms			
Verify that systems capable of audit have auditing enabled or if the system is incapable of audit, the GCA has provided contract documentation that clearly directs the use of those operating systems. (NISPOM 8-602, ISL 2007-01, Q41)	☐	☐	☐
Verify the system is recording successful and unsuccessful logons and logoffs. (NISPOM 8-602a(1)(b))	☐	☐	☐
Verify the system is recording unsuccessful attempts to access security relevant files and directories. (NISPOM 8-602a(1)(c))	☐	☐	☐
Verify the system is recording denial of system access (account lockout) due to multiple failed login attempts. (NISPOM 8-602a(1)(f))	☐	☐	☐
Verify the system is recording changes to passwords. (NISPOM 8-602a(1)(d))	☐	☐	☐
Verify that the audit records generated by the system contain the following information: date and time of the action, type of action, and the responsible person for the action, and the resources involved (e.g. name of file for a failed access attempt of a file). (NISPOM 8-602a(1)(a))	☐	☐	☐
Virus Detection and Malicious Code			
Verify that virus detection software has been installed, is functional, and has been executed on all installed media. (NISPOM 8-305)	☐	☐	☐
Verify that all IS software has been tested for malicious code as feasible. (NISPOM 8-305)	☐	☐	☐
Sanitization Procedures			
Verify all sanitization procedures have been validated. (NISPOM 8-301 and DSS Clearing and Sanitization Matrix)	☐	☐	☐
Trusted Download Procedure			
Verify that trusted download procedures are in accordance with DSS procedures and formats or that the GCA has acknowledged the Risk via DD254, contract, or memorandum. (NISPOM 8-310b)	☐	☐	☐
Networks			
Transmission: Verify transmission is through a Protected Distribution System or by use of an NSA Type 1 Encryptor. (NSTISSI 7003)	☐	☐	☐
Interconnected network: Verify security policy is in accordance with the DSS Approved Network Security Plan. (NISPOM 8-700)	☐	☐	☐
Interconnected network: If connected to a government system, verify security policy is in accordance with MOU. (NISPOM 8-700)	☐	☐	☐

☒ This page is not applicable

Operating System(s):	**Version(s):**

Accounts, Logons, and Session Controls

Identification & Authentication (I&A) is technically enforced: ☐Yes ☐No If No, Users will manually record User Access, Refer to Attachment:

Password generation routine: ☐ IS generated random password ☐Passwords assigned by administrator ☐User generated passwords

Check if Technically Enforceable: ☐ Password Length ☐ Password Complexity

Password lifetime (# of days):

Periods processing: ☐No ☐Yes* (Explain procedures in addl info/comments section at end of document.)

Lockouts for multiple failed logins: ☐ Yes, After attempts and ☐ After minutes and\or ☐ an administrator is required to unlock the account.

I&A Management: Describe how User IDs & Passwords are established and distributed:

User Accounts will be validated annually by: ☐ System Administrator ☐ ISSM ☐ ISSO ☐ Other, Specify:

Generic or Group accounts: ☐ No ☐ Yes* If yes, list each group account (group authorization) on IS, with a justification for their use:

Account Name: Justification:

Account Name: Justification:

Account Name: Justification:

*When group accounts are used, manual logs (or other methods) should be utilized to assure individual accountability.

System Audit Capabilities

Automated Audit Trails: ☐ No ☐ Yes If yes, Identify Audit Mechanism:	**Audit Capabilities -** Check all that are technically feasible and enabled: ☐ Successful Logons ☐ Unsuccessful logons ☐ Logoffs ☐ Denial of System access due to failed logins ☐ Unsuccessful access to objects ☐ Changes in Passwords

Audit Management:

Automated audit records are maintained: ☐ Locally to each system ☐ Offline via media

Audit overflow configuration: ☐ System will shutdown

Retention period for online audit records: Retention period for offline audit records:

Description of IS Records and Logs:

In addition to the automated logs generated by the system, records and logs of IS

☐ All records and logs are generated and maintained manually in hardcopy form, examples are attached

☐ Some IS changes or actions are recorded within online automated systems. Describe:

Virus and Malicious Code Detection	**Access Controls to Security Relevant Objects**
Virus Detection Software Installed: ☐Yes ☐No If yes, how often are signature files updated: If No, Alternate method:	This IS is capable of file permissions or ACLs: ☐Yes ☐No

☒ This page is not applicable

ISSM System Certification Test Checklist	
Facility Name:	**IS#:**

Instructions: Most protection measures on this page are implemented through IS technical controls. This portion of the certification test guide must be filled out for each platform contained on the system (e.g. Windows 2000, Sun Solaris 8.0). Verify all technical controls are in place and operating correctly. **S** denotes the results for a particular technical control are in place and operating successfully. **F** denotes the technical control is not in place or the verification test failed**. All failed results must have a corrective action taken prior to certifying the IS.** Specify **N/A** if the particular technical control does not apply to this IS (for example, a single user standalone does not require technical audit controls and verification may be N/A).

Profile Version#:	**Operating System:**	**O/S Version #:**

	N/A	S	F
Logon Authentication			
Technical Implementation: If logon authentication is technically implemented, verify that IS users are required to present their User ID and authenticator to gain access (NISPOM 8-303)	☐	☐	☐
If user access is not technically implemented through logon authentication (single user standalones), verify physical security controls and personnel security controls such as an Authorized User List are sufficient. (NISPOM 8-303c)	☐	☐	☐
Session Controls			
Technical Implementation: Verify the DSS or contractually required logon banner is displayed on all systems and that the user is required to take positive action to remove the notice from the screen. (NISPOM 8-609a(1))	☐	☐	☐
If the warning banner is not technically implemented, verify it is prominently displayed in the area or other methods of notification are developed and approved by DSS. (NISPOM 8-609a(1)).	☐	☐	☐
If the OS is capable, verify that successive logon attempts are controlled by: denying access after multiple consecutive unsuccessful access attempts of the same user ID, limiting number of access attempts within a time period, by use of a time delay control. (NISPOM 8-609(2))	☐	☐	☐
Verify system entry granted only in accordance with user's profile and if not explicitly granted, verify all remote activities such as remote logons and anonymous file accesses are prohibited. (NISPOM 8-609(3))	☐	☐	☐
Password Controls			
Verify that when passwords are entered they are not visible (must be masked). (NISPOM 8-303i(4))	☐	☐	☐
Password Generation: If the IS generates the passwords, verify the IS generates a random password that is a minimum of 14 non-blank characters. (NISPOM 8-303i(2))	☐	☐	☐
If passwords are User generated, verify the following features, as specified in the profile, are properly functioning: Minimum password length (14-characters), Password composition (mixture of characters/numbers, and upper/lower case) Capability to require a password change upon reaching the allowed password lifetime. (NISPOM 8-303i)	☐	☐	☐
If present, verify that vendor standard accounts with pre-defined passwords have been changed or disabled. Verify that they have also been changed or disabled after a new system version is installed or other action initiated that might result in restoration of these passwords/accounts. (NISPOM 8-303i(5))	☐	☐	☐
Group Accounts: If group authenticators are used, verify they are used in association with individual authenticators. (NISPOM 8-607b and 8-505)	☐	☐	☐
If present, verify that the BIOS setup, EEPROM access or single user mode, GRUB or LILO loader is password protected. (NISPOM 8-613a(1))	☐	☐	☐
Access Protections			
Verify that the file(s) containing passwords is either not accessible to non-privileged users, or that the passwords are encrypted. (NISPOM 8-303d)	☐	☐	☐
Verify that the file(s) containing audit data is not accessible to non-privileged users. (NISPOM 8-602a(2))	☐	☐	☐

☒ This page is not applicable

Verify the files and directories that control the system and/or its security may not be modified or deleted by non-privileged users. (NISPOM 8-613)	☐	☐	☐
Verify that writing to floppy drives, CD-ROM drives, or use of USB drives, not expressly permitted by the security policy are prohibited. (NISPOM 8-609a(3) and 8-606)	☐	☐	☐
Verify that security procedures are in place to mitigate risks inherent with wireless devices. (NISPOM 1-200 and ISL 2006-02, Q1)	☐	☐	☐
Audit Mechanisms			
Verify that systems capable of audit have auditing enabled or if the system is incapable of audit, the GCA has provided contract documentation that clearly directs the use of those operating systems. (NISPOM 8-602, ISL 2007-01, Q41)	☐	☐	☐
Verify the system is recording successful and unsuccessful logons and logoffs. (NISPOM 8-602a(1)(b))	☐	☐	☐
Verify the system is recording unsuccessful attempts to access security relevant files and directories. (NISPOM 8-602a(1)(c))	☐	☐	☐
Verify the system is recording denial of system access (account lockout) due to multiple failed login attempts. (NISPOM 8-602a(1)(f))	☐	☐	☐
Verify the system is recording changes to passwords. (NISPOM 8-602a(1)(d))	☐	☐	☐
Verify that the audit records generated by the system contain the following information: date and time of the action, type of action, and the responsible person for the action, and the resources involved (e.g. name of file for a failed access attempt of a file). (NISPOM 8-602a(1)(a))	☐	☐	☐
Virus Detection and Malicious Code			
Verify that virus detection software has been installed, is functional, and has been executed on all installed media. (NISPOM 8-305)	☐	☐	☐
Verify that all IS software has been tested for malicious code as feasible. (NISPOM 8-305)	☐	☐	☐
Sanitization Procedures			
Verify all sanitization procedures have been validated. (NISPOM 8-301 and DSS Clearing and Sanitization Matrix)	☐	☐	☐
Trusted Download Procedure			
Verify that trusted download procedures are in accordance with DSS procedures and formats or that the GCA has acknowledged the Risk via DD254, contract, or memorandum. (NISPOM 8-310b)	☐	☐	☐
Networks			
Transmission: Verify transmission is through a Protected Distribution System or by use of an NSA Type 1 Encryptor. (NSTISSI 7003)	☐	☐	☐
Interconnected network: Verify security policy is in accordance with the DSS Approved Network Security Plan. (NISPOM 8-700)	☐	☐	☐
Interconnected network: If connected to a government system, verify security policy is in accordance with MOU. (NISPOM 8-700)	☐	☐	☐

☒ This page is not applicable

Operating System(s):	**Version(s):**

Accounts, Logons, and Session Controls

Identification & Authentication (I&A) is technically enforced: ☐ Yes ☐ No If No, Users will manually record User Access, Refer to Attachment:

Password generation routine: ☐ IS generated random password ☐ Passwords assigned by administrator ☐ User generated passwords

Check if Technically Enforceable: ☐ Password Length ☐ Password Complexity

Password lifetime (# of days):

Periods processing: ☐ No ☐ Yes* (Explain procedures in addl info/comments section at end of document.)

Lockouts for multiple failed logins: ☐ Yes, After attempts and ☐ After minutes and\or ☐ an administrator is required to unlock the account.

I&A Management: Describe how User IDs & Passwords are established and distributed:

User Accounts will be validated annually by: ☐ System Administrator ☐ ISSM ☐ ISSO ☐ Other, Specify:

Generic or Group accounts: ☐ No ☐ Yes* If yes, list each group account (group authorization) on IS, with a justification for their use:

Account Name: Justification:

Account Name: Justification:

Account Name: Justification:

*When group accounts are used, manual logs (or other methods) should be utilized to assure individual accountability.

System Audit Capabilities

Automated Audit Trails: ☐ No ☐ Yes If yes, Identify Audit Mechanism:	**Audit Capabilities -** Check all that are technically feasible and enabled: ☐ Successful Logons ☐ Unsuccessful logons ☐ Logoffs ☐ Denial of System access due to failed logins ☐ Unsuccessful access to objects ☐ Changes in Passwords

Audit Management:

Automated audit records are maintained: ☐ Locally to each system ☐ Offline via media

Audit overflow configuration ☐ System will shutdown

Retention period for online audit records: Retention period for offline audit records:

Description of IS Records and Logs:

In addition to the automated logs generated by the system, records and logs of IS

☐ All records and logs are generated and maintained manually in hardcopy form, examples are attached

☐ Some IS changes or actions are recorded within online automated systems. Describe:

Virus and Malicious Code Detection	**Access Controls to Security Relevant Objects**
Virus Detection Software Installed: ☐ Yes ☐ No If yes, how often are signature files updated: If No, Alternate method:	This IS is capable of file permissions or ACLs: ☐ Yes ☐ No

☒ This page is not applicable

ISSM System Certification Test Checklist	
Facility Name:	**IS#:**

Instructions: Most protection measures on this page are implemented through IS technical controls. This portion of the certification test guide must be filled out for each platform contained on the system (e.g. Windows 2000, Sun Solaris 8.0). Verify all technical controls are in place and operating correctly. **S** denotes the results for a particular technical control are in place and operating successfully. **F** denotes the technical control is not in place or the verification test failed**. All failed results must have a corrective action taken prior to certifying the IS.** Specify **N/A** if the particular technical control does not apply to this IS (for example, a single user standalone does not require technical audit controls and verification may be N/A).

Profile Version#:	**Operating System:**	**O/S Version #:**

	N/A	S	F
Logon Authentication			
Technical Implementation: If logon authentication is technically implemented, verify that IS users are required to present their User ID and authenticator to gain access (NISPOM 8-303)	☐	☐	☐
If user access is not technically implemented through logon authentication (single user standalones), verify physical security controls and personnel security controls such as an Authorized User List are sufficient. (NISPOM 8-303c)	☐	☐	☐
Session Controls			
Technical Implementation: Verify the DSS or contractually required logon banner is displayed on all systems and that the user is required to take positive action to remove the notice from the screen. (NISPOM 8-609a(1))	☐	☐	☐
If the warning banner is not technically implemented, verify it is prominently displayed in the area or other methods of notification are developed and approved by DSS. (NISPOM 8-609a(1)).	☐	☐	☐
If the OS is capable, verify that successive logon attempts are controlled by: denying access after multiple consecutive unsuccessful access attempts of the same user ID, limiting number of access attempts within a time period, by use of a time delay control. (NISPOM 8-609(2))	☐	☐	☐
Verify system entry granted only in accordance with user's profile and if not explicitly granted, verify all remote activities such as remote logons and anonymous file accesses are prohibited. (NISPOM 8-609(3))	☐	☐	☐
Password Controls			
Verify that when passwords are entered they are not visible (must be masked). (NISPOM 8-303i(4))	☐	☐	☐
Password Generation: If the IS generates the passwords, verify the IS generates a random password that is a minimum of 14 non-blank characters. (NISPOM 8-303i(2))	☐	☐	☐
If passwords are User generated, verify the following features, as specified in the profile, are properly functioning: Minimum password length (14-characters), Password composition (mixture of characters/numbers, and upper/lower case) Capability to require a password change upon reaching the allowed password lifetime. (NISPOM 8-303i)	☐	☐	☐
If present, verify that vendor standard accounts with pre-defined passwords have been changed or disabled. Verify that they have also been changed or disabled after a new system version is installed or other action initiated that might result in restoration of these passwords/accounts. (NISPOM 8-303i(5))	☐	☐	☐
Group Accounts: If group authenticators are used, verify they are used in association with individual authenticators. (NISPOM 8-607b and 8-505)	☐	☐	☐
If present, verify that the BIOS setup, EEPROM access or single user mode, GRUB or LILO loader is password protected. (NISPOM 8-613a(1))	☐	☐	☐
Access Protections			
Verify that the file(s) containing passwords is either not accessible to non-privileged users, or that the passwords are encrypted. (NISPOM 8-303d)	☐	☐	☐
Verify that the file(s) containing audit data is not accessible to non-privileged users. (NISPOM 8-602a(2))	☐	☐	☐

☒ This page is not applicable

Verify the files and directories that control the system and/or its security may not be modified or deleted by non-privileged users. (NISPOM 8-613)	☐	☐	☐
Verify that writing to floppy drives, CD-ROM drives, or use of USB drives, not expressly permitted by the security policy are prohibited. (NISPOM 8-609a(3) and 8-606)	☐	☐	☐
Verify that security procedures are in place to mitigate risks inherent with wireless devices. (NISPOM 1-200 and ISL 2006-02, Q1)	☐	☐	☐
Audit Mechanisms			
Verify that systems capable of audit have auditing enabled or if the system is incapable of audit, the GCA has provided contract documentation that clearly directs the use of those operating systems. (NISPOM 8-602, ISL 2007-01, Q41)	☐	☐	☐
Verify the system is recording successful and unsuccessful logons and logoffs. (NISPOM 8-602a(1)(b))	☐	☐	☐
Verify the system is recording unsuccessful attempts to access security relevant files and directories. (NISPOM 8-602a(1)(c))	☐	☐	☐
Verify the system is recording denial of system access (account lockout) due to multiple failed login attempts. (NISPOM 8-602a(1)(f))	☐	☐	☐
Verify the system is recording changes to passwords. (NISPOM 8-602a(1)(d))	☐	☐	☐
Verify that the audit records generated by the system contain the following information: date and time of the action, type of action, and the responsible person for the action, and the resources involved (e.g. name of file for a failed access attempt of a file). (NISPOM 8-602a(1)(a))	☐	☐	☐
Virus Detection and Malicious Code			
Verify that virus detection software has been installed, is functional, and has been executed on all installed media. (NISPOM 8-305)	☐	☐	☐
Verify that all IS software has been tested for malicious code as feasible. (NISPOM 8-305)	☐	☐	☐
Sanitization Procedures			
Verify all sanitization procedures have been validated. (NISPOM 8-301 and DSS Clearing and Sanitization Matrix)	☐	☐	☐
Trusted Download Procedure			
Verify that trusted download procedures are in accordance with DSS procedures and formats or that the GCA has acknowledged the Risk via DD254, contract, or memorandum. (NISPOM 8-310b)	☐	☐	☐
Networks			
Transmission: Verify transmission is through a Protected Distribution System or by use of an NSA Type 1 Encryptor. (NSTISSI 7003)	☐	☐	☐
Interconnected network: Verify security policy is in accordance with the DSS Approved Network Security Plan. (NISPOM 8-700)	☐	☐	☐
Interconnected network: If connected to a government system, verify security policy is in accordance with MOU. (NISPOM 8-700)	☐	☐	☐

☒ This page is not applicable

Additional information/comments:

☒ This page is not applicable

Additional information/comments:

☒ This page is not applicable

This page is for the uploading of scanned images (signed DSS 147, additional network diagrams, etc.).

☒ This page is not applicable

This page is for the uploading of scanned images (signed DSS 147, additional network diagrams, etc.).